

IN THE CLAIMS

1. (Currently Amended) A method of securely providing content data to a user's system over a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:

encrypting ~~the~~content data using a first encrypting key to form encrypted content data, wherein the first encrypting key is a symmetric key;

encrypting the first decrypting key, using a second encrypting key;

broadcasting promotional metadata related to at least part of the encrypted content data on a first web broadcast channel for reception by at least one user's system;

~~broadcasting~~sending at least part of the encrypted content data over a second broadcast channel, ~~wherein at least the second broadcast channel is not encrypted~~; and

transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key, to the user's system via a computer readable medium; and

decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with a second decrypting key;

wherein the tamper resistant environment forms reencrypted content data by decrypting the encrypted content data with the first decrypting key and reencrypting the content data with a locally generated digital content player encrypting key so to be compatible with a content player application on the user's system which renders reencrypted content data delivered from one of a telecommunications infrastructure and a computer readable storage medium.

2. (Original) The method as defined in claim 1, wherein the step of broadcasting the promotional metadata includes broadcasting the promotional metadata periodically over a predetermined time interval.

3. (Currently Amended) The method as defined in claim 1, wherein the step of broadcasting the promotional metadata includes the sub-step of:

converting at least the promotional metadata into a format readable by a web browser[;].

4. (Currently Amended) The method as defined in claim 1, wherein the step of broadcastingsending at least part of the encrypted content data includes broadcasting a schedule of ~~the~~ broadcast time and web broadcast channel for at least part of the encrypted content data;

5. (Currently Amended) The method as defined in claim 1, wherein the step of broadcastingsending at least part of the encrypted content data over a second web broadcast channel includes broadcasting the encrypted content data in a format compatible with DirecPC™.

6. (Currently Amended) The method as defined in claim 1, wherein the promotional metadata contains a schedule of broadcast times for the encrypted content data.

7. (Currently Amended) A method of securely receiving content data on a user's system from a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:
receiving promotional metadata from a first web broadcast channel, the promotional metadata related to encrypted content data available for reception;

assembling at least part of the promotional metadata into a promotional offering for review by a user;

selecting by a user, encrypted content data to be received related to the promotional offering metadata;

~~receiving~~ retrieving the encrypted content data from a user's system via a second web broadcast channel, the encrypted content data selected from the promotional metadata, and wherein the encrypted content data has been previously encrypted using a first encrypting key, wherein the first encrypting key is a symmetric key and ~~wherein at least the second web broadcast channel is not encrypted, wherein the second channel is selected from the group consisting of a telecommunications network, a broadcast transmission, and a computer removable storage medium; and~~

receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the encrypted content data received via the second web broadcast channel; and

decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with a second decrypting key;

wherein the tamper resistant environment forms reencrypted content data by decrypting the encrypted content data with the first decrypting key and reencrypting the content data with a locally generated digital content player encrypting key so to be compatible with a content player application on the user's system which renders reencrypted content data delivered from one of a telecommunications infrastructure and a computer readable storage medium.

8. (Original) The method as defined in claim 7, wherein the step of assembling at least part of the promotional data includes assembling at least part of the promotional data into a format readable by a web browser and wherein the step of selecting includes selecting with a web browser.

9. (Currently Amended) The method as defined in claim 7, wherein the step of selecting includes selecting promotional material that ~~have~~has been previously received and stored on the user's system.

10. (Currently Amended) The method as defined in claim 9, wherein the step of selecting further comprises the sub-steps of:

determining ~~the~~a schedule for ~~the~~a next web broadcast of the encrypted content data selected;

setting a trigger to trigger the user's system to receive the next web broadcast on the second channel.

11. (Currently Amended) The method as defined in claim 10, wherein the step of ~~receiving~~retrieving encrypted content data from a second ~~web broadcast channel~~, includes receiving the encrypted content data selected from the promotional metadata on a web broadcast channel and a time provided by the trigger.

12. (Currently Amended) The method as defined in claim 7, wherein the step of ~~receiving~~retrieving encrypted content data from a second ~~web-broadcast-channel~~ includes receiving data in a format compatible with DirecPC™.

13. (Currently Amended) The method as defined claim 7, wherein the step of receiving data from a second ~~web-broadcast-channel~~ includes the sub-step of:

authorizing over a back channel that the user's system is authorized to receive the data selected; and wherein the step of receiving the first decrypting key includes receiving the first decrypting key only if the user's system is authorized to receive the encrypted content data selected.

91 14. (Currently Amended) The method as defined claim 7, wherein the step of receiving encrypted content data from a second ~~web-broadcast-channel~~ further includes the sub-step of:

notifying the user the next time the user starts the user's system a status if the current data selected from the promotional metadata has been received on the user's system.

15. (Original) The method as defined in claim 7, wherein the step of receiving the first decrypting key, includes receiving the first decrypting key that has been encrypted with a second encrypting key.

16. (Original) The method as defined in claim 15, wherein the step of receiving the first decrypting key includes receiving the first decrypting key over a broadcast stream.

17. (Original) The method defined in claim 15, wherein the second decrypting key is sent to the user's system from a clearinghouse.

18. (Original) The method defined in claim 15, wherein the second decrypting key has a timeout provision for decrypting data that has been encrypted with the second encryption key is sent to the user's system from a clearinghouse.

19. (Currently Amended) A system for securely providing content data to a user's system over a web broadcast infrastructure with a plurality of channels, the system comprising:

a content system;

a first public key;

a first private key, which corresponds to the first public key;

a data encrypting key;

a data decrypting key for decrypting data encrypted using the data encrypting key,

wherein the first encrypting key is a symmetric key;

first data encryption means for encrypting data to form encrypted content data so as to be decryptable only by the data decrypting key;

second data encryption means, using the first public key, for encrypting the data decrypting key;

a clearing house;

91
a broadcast center, for broadcasting to one or more user's systems on a first web broadcast channel, promotional metadata related to data being broadcasted on a second web broadcast channel, and broadcastingsending on the second broadcast channel encrypted content data encrypted with the data encrypting key, and wherein at least the second broadcast channel is not encrypted, wherein the second channel is selected from the group consisting of a telecommunications network, a broadcast transmission, and a computer removable storage medium;

first transferring means for transferring the data decrypting key which has been encrypted, to the clearing house, wherein the clearinghouse possesses the first private key;

first decrypting means for decrypting the data decrypting key using the first private key;

a second public key;

a second private key, which corresponds to the second public key;

re-encryption means for re-encrypting the data decrypting key using the second public key;

second transferring means for transferring the re-encrypted data decrypting key to the user's system, wherein the user's system possesses the second private key; and

second decrypting means for decrypting the re-encrypted data decrypting key using the second private key; and

decrypting, on the user's system in a tamper resistant environment, the encrypted data decrypting key with the first private key;

wherein the tamper resistant environment forms reencrypted content data by decrypting the encrypted content data with the data decrypting key and reencrypting the content data with a locally generated digital content player encrypting key so to be compatible with a content player application on the user's system which renders reencrypted content data delivered from one of a telecommunications infrastructure and a computer readable storage medium.

20. (Original) The system as defined in claim 19, wherein the promotional metadata contains a schedule of broadcast times for the data.

21. (Currently Amended) A user's system for securely receiving data from a web broadcast infrastructure with a plurality of channels, comprising:

a receiver for receiving promotional metadata from a first web broadcast channel, the promotional metadata related to data available for reception;

an interface to an output device for presenting at least part of the promotional metadata for review by a user;

an interface to an input device for receiving a selection by a user of the data to be received related to the promotional metadata;

a controller for controlling the receiver to receive data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key, wherein the first encrypting key is a symmetric key and wherein at least the second broadcast channel is not encrypted, wherein the second channel is selected from the group consisting of a telecommunications network, a broadcast transmission, and a computer removable storage medium; and

an interface for receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web

broadcast channel;

decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with the second decrypting key,

wherein the tamper resistant environment forms reencrypted content data by reencrypting the content data with a locally generated digital content player encrypting key;

wherein the previously encrypted content data has been decrypted with the first decrypting key, and the tamper resistant environment storing the reencrypted content data on storage device coupled to the user's system is compatible with a player application used to render the reencrypted content data delivered from one of a telecommunications infrastructure and a computer readable storage medium.

22. (Original) The user's system as defined in claim 21, wherein the output device is a web browser and the input device is coupled to the web browser for receiving a selection by a user.

23. (Original) The user's system as defined in claim 21, wherein the controller further comprises:
a schedule derived from the promotional metadata wherein the schedule is used to control the receiver to receive data from a second web broadcast channel.


24. (Original) The user's system as defined in claim 21, wherein the receiver is adapted to receive data broadcasted in a format compatible with DirecPC™.

25. (New) A computer program product for securely providing content data to a user's system over a web broadcast infrastructure with a plurality of channels, the computer program product comprising:

a storage medium readable by a processing circuit and storing instructions for execution by the processing circuit for performing a method comprising:

encrypting content data using a first encrypting key to form encrypted content data, wherein the first encrypting key is a symmetric key;

encrypting the first decrypting key, using a second encrypting key;



broadcasting promotional metadata related to at least part of the encrypted content data on a first web broadcast channel for reception by at least one user's system;
sending at least part of the encrypted content data over a second channel;
transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key, to the user's system via a computer readable medium; and
decrypting, on the user's system in a tamper resistant environment, the encrypted first decrypting key with a second decrypting key;

wherein the tamper resistant environment forms reencrypted content data by decrypting the encrypted content data with the first decrypting key and reencrypting the content data with a locally generated digital content player encrypting key so to be compatible with a content player application on the user's system which renders reencrypted content data delivered from one of a telecommunications infrastructure and a computer readable storage medium.
